УДК 623.1/7

ОРГАНИЗАЦИЯ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ В КСА

Кнауб Е.В.,
научный руководитель доцент Троценко Л. С.
Сибирский Федеральный Университет

Одним из приоритетных направлений развития науки в России в настоящий момент является внедрение информационных технологий во все сферы исследований и жизнедеятельности человека. Эти технологии призваны коренным образом изменить темпы развития в третьем тысячелетии и подходы к решению фундаментальных и прикладных проблем, стоящих перед учеными. Очевидно, что в перспективе производство и использование информации будет занимать центральное место в организации всей общественной жизни. Можно говорить о назревающей тенденции к формированию общества, характерной чертой которого станет доступность знаний, не ограниченная пространством и временем, социальными и иными барьерами.

Исключение не составляют и Вооруженные Силы Российской Федерации. В настоящее время Управлением начальника связи Вооруженных Сил РФ развернута активная работа по реализации концепции создания единого информационного пространства ВС РФ, что должно способствовать эффективному применению войск (сил) путем организации своевременного планирования и согласования их действий, обеспечения своевременной обратной связи с подчиненными соединениями, частями и подразделениями для получения сведений об их состоянии, положении и средствах, способствующих выполнению поставленных задач.

При этом фундаментом такой системы будет выступать глобальная (пространственно-разнесенная) информационная сеть, создаваемая на базе имеющихся и перспективных сетей связи и передачи данных (на основе применения современных телекоммуникационных технологий) и обладающая высокими оперативно-техническими характеристиками. Такая сеть должна обеспечить непрерывный и единообразный обмен информацией для всех систем и средств, используемых в мирное время и при ведении боевых действий.

Другим важным направлением является обеспечение широкомасштабной автоматизации управления войсками во всех звеньях и создание средств, позволяющих формировать единую картину «поля боя» на основе получаемой от различных источников информации, доводить ее до руководства в удобном для принятия решения виде, а также обеспечивать планирование боевого применения войск (сил) и оружия в близком к реальному масштабу времени.

Актуальность исследования. В настоящее время при проектировании данной системы проблемы обеспечения информационной безопасности стали играть ключевую роль. Так, например, в КСА КП РТВ хранится множество секретных данных, утечка которых понесет не только уголовное наказание конкретному лицу, но и угрозу безопасности всей страны в целом.

Управление доступом должно учитывать, с одной стороны, как наличие штатных средств реализации механизмов обеспечения безопасности (механизмы, встроенные в операционные среды и прикладные системы), так и наличие различных уровней управления - персональный, региональный и федеральный.

Таким образом, тема работы является актуальной и непосредственно связана с глобальной проблемой управления техническим циклом жизни программно-технических изделий (в данном случае относящихся к обеспечению безопасности КСА).

Цель работы - разработка информационной системы управления доступом для современных КСА.

Реализация данной системы позволить увеличить безопасность данных в системе КСА и свести к минимуму утечку секретной информации.

Модель управления доступом – это структура, которая определяет порядок доступа субъектов к объектам. Для реализации правил и целей этой модели используются технологии управления доступом и механизмы безопасности.

На данных момент в Вооруженных Силах РФ, а точнее, в КСА ПУ РТВ используется модель принудительного контроля доступа, принципиальным отличием которой является то, что права доступа определяются единым централизованным органом администрирования с правами суперпользователя и не могут быть переопределены обычными пользователями.

Данная информационная система предполагает управление доступом на основе ролей, основная идея которой построена на максимальном приближении логики работы системы к реальному разделению функций пользователей.

Ролевой метод управления доступом контролирует доступ пользователей к информации на основе типов их активностей в системе. Применение этого метода подразумевает определение ролей в системе. Понятие роль определяется как совокупность действий и обязанностей, связанных с определенным видом деятельности. Следовательно, вместо того, чтобы указывать все типы доступа для каждого пользователя к каждому объекту, достаточно указать тип доступа к объектам для роли. А пользователям, в свою очередь, указать их роли. Пользователь, "выполняющий" роль, имеет доступ определенный для роли.

Обобщая, можно сказать, что пользователь может выполнять различные роли в разных ситуациях. А одна и та же роль может быть использована несколькими различными пользователями, причем в некоторых случаях даже одновременно.

В классических моделях разграничения доступа, права на выполнение определенных операций над объектом описываются для каждого пользователя или группы пользователей. В ролевой модели дифференциация понятий роль и пользователь позволяет разбить задачу на две части: определение роли пользователя и определение прав доступа к объекту для роли. Такой подход значительно упрощает процесс администрирования, так как для изменения области ответственности пользователя, достаточно удалить старые роли и определить новые соответствующие его измененным обязанностям.

Системы с ролевым управлением доступом целесообразно использовать в больших организациях, со сложной иерархией и большим количеством разделяемых операций. В такой системе данные принадлежат конкретному не пользователю, а системе в общем. Следовательно, эта модель намного больше подходит для КСА.

Реализацией данного проекта является комплексная система, представляющая собой визуально наглядную оболочку для управления, редактирования, тестирования системы.

Разрабатываемая информационная система управления доступом обеспечит выполнение следующих функций:

1. идентификация, т.е. присвоение уникальных признаков - идентификаторов, по которым в дальнейшем система производит аутентификацию;
2. аутентификация, т.е. установление подлинности на основе сравнения с эталонными идентификаторами;
3. разграничение доступа пользователей к ПЭВМ;

4. разграничение доступа пользователей по операциям над ресурсами (программы, данные и т.д.);
5. администрирование:
   a. определение прав доступа к защищаемым ресурсам,
   b. обработка регистрационных журналов,
   c. установка системы защиты на ПЭВМ,
   d. снятие системы защиты с ПЭВМ;
6. регистрация событий:
   a. входа пользователя в систему,
   b. выхода пользователя из системы,
   c. нарушения прав доступа;
7. реакция на попытки несанкционированного доступа;
8. контроль целостности и работоспособности систем защиты;
9. обеспечение информационной безопасности при проведении ремонтно-профилактических работ;
10. обеспечение информационной безопасности в аварийных ситуациях.